

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

In re the Application

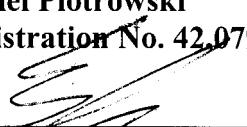
Inventor : **Jin Lu et al.**
Application No. : **09/461,984**
Filed : **December 15, 1999**
For : **SYSTEM AND METHOD FOR COPY PROTECTING
TRANSMITTED INFORMATION**

APPEAL BRIEF

On Appeal from Group Art Unit 2136

Date: March 23, 2007

Daniel Piotrowski
Registration No. 42,079



By: Steve Cha
Attorney for Applicant
Registration No. 44,069

TABLE OF CONTENTS

	<u>Page</u>
I. REAL PARTY IN INTEREST.....	3
II. RELATED APPEALS AND INTERFERENCES.....	3
III. STATUS OF CLAIMS.....	3
IV. STATUS OF AMENDMENTS.....	3
V. SUMMARY OF CLAIMED SUBJECT MATTER.....	3
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL.....	5
VII. ARGUMENT.....	5
VIII. CONCLUSION	9
IX. CLAIMS APPENDIX.....	10
X. EVIDENCE APPENDIX.....	17
XI. RELATED PROCEEDINGS APPENDIX.....	17

TABLE OF CASES

<i>In re Vaeck</i> , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)	7
<i>Ex parte Levensgood</i> , 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993) .	9
<i>In re Fine</i> , 837 F.2d 1071, 5 USPQ 2d 1596 (Fed. Cir. 1988)	10

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, U.S. Philips Corporation, and not the party named in the above caption.

II. RELATED APPEALS AND INTERFERENCES

With regard to identifying by number and filing date all other appeals or interferences known to Appellant which will directly effect or be directly affected by or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-30 have been presented for examination. All of these claims are pending, stand finally rejected, and form the subject matter of the present appeal.

IV. STATUS OF AMENDMENTS

The Amendment after the Final Office Action has been entered. No amendments were made to the claims in Appellant's response to the rejection of the claims in the Final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The instant application recites in independent claim 1, a system, in independent claim 2, a method, in independent claim 8, a module, in independent claim 13, a host device, and in independent claim 18, an article of manufacture for copy protecting

information. The remaining claims depend from the independent claims and recite further aspects of the invention claimed.

Claim 1, which is typical of the remaining independent claims, recites a point of deployment module (POD) and a set-top box (see page 6, lines 12-15) the set-top box generates a request for content information (see page 9, lines 1-11) and in response the POD generates a reply message that includes at least one control information pair having copy control information and a stream identifier (see page 9, lines 23-26), the set-top box and POD generate keys that are shared by both devices using the control information pair (see page 9, line 2- page 10, 30), the POD then encrypts the information with a first one of the shared keys (see page 12, lines 12-15) and the set-top box decrypts the encrypted information with a second one of the shared keys generated by the set-top box (see page 12, lines 16-19).

Independent claim 2 recites a method of copy protecting information transmitted between a deployment module and a host device, the deployment module in response to a request by the host device, generating a reply message that includes at least one control information pair including copy control information and a steam identifier, encrypting the information using a key generated from at least the control information pair at the deployment module and the host device decrypting the encrypted information using a key generated at the host device. Independent claim 8 recites a deployment module performing the operations associated with the system described in independent claim 1. Independent claim 13 recites a host device performing the operations associated with the system described in independent claim 1. Independent claim 18 recites a computer

program providing instructions for performing the operations of the system described in independent claim 1.

The remaining dependent claims recite further aspects of the invention recited in the independent claims.

VI. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are whether:

1. Claims 1-30 are unpatentable under 35 USC §103(a) over the combination of Zhang (USP no. 6,550,008) in view of Applicant's Admitted Prior Art (AAPA) and further in view of Sawabe (USP no. 6,571,055).

VII. ARGUMENT

Claims 1-30 stand rejected under 35 USC 103(a) as being unpatentable in view of the combination of Zhang, AAPA and Sawabe. The Final Office Action states that Zhang teaches the elements of claim 1, but fails to teach "the reply message includes at least one control information pair, each control information pair having copy control information and a stream identifier and the keys are generated using at least one control information pair." The Final Office Action further refers to AAPA for teaching "one control information pair, each having a copy control information and a stream identifier" and Sawabe for teaching the keys are generated using the at least one control information pair. In maintaining the rejection of the claims, the Advisory Action states that the "AAPA was cited for teaching this limitation, mainly page 2, last paragraph, which describes every copy protected elementary stream having an associated copy control

information. An elementary stream contains a stream identifier and a copy protected elementary stream contains a copy control information and a stream identifier." (see AA, page 2).

Rejection of Claim 1 under 35 USC §103

The rejection of claim 1 is in error because the references fail to show a limitation cited therein.

Zhang teaches a method and apparatus for protecting information communicated between a first and second device, which includes generating a request to a third device. The request includes information identifying the first and second devices. The third device verifies the first and second devices based on the information in the request. Predetermined information is sent to at least one of the first and second devices and the first and second devices authenticate each other based on the predetermined information. (see Abstract). Zhang discloses that in some embodiments "the invention employs a trusted third party that is able to pass either the public key or secret keys of the one or more host devices and POD modules ..." (see col. 4, lines 38-41).

The AAPA is a standards document for telecommunications. The AAPA includes a 7-bit field in the PES header that allows for "additional copy info." However, the AAPA fails to disclose that a stream identifier is to be stored in the 7-bit field and that the stream identifier is to be used for additional copy info. (see page 11-12).

Sawabe discloses recording information that comprises a plurality of information units each including heading information and divided-compressed audio information obtained by dividing compressed audio information so as to include one or a plurality of lead data positioned at a [head] of compressed partial audio information. (see Abstract).

Sawabe discloses, in fig. 2, which is referred to in the Final Office Action, that a packet includes a stream ID 241b and copy information 241d. However, Sawabe fails to provide any teaching with regard to the further use of the stream ID or the copy information.

Applicant believes that Sawabe is recited to show that the stream ID may be included in the 7-bits of the "additional copy info" field referred to by AAPA and that Zhang may then use the additional copy info to generate session keys. However, neither Zhang nor Sawabe teach or suggest the use of a stream id for determining the session keys, as is recited in the claims.

In order to establish a *prima facie* case of obviousness, three basic criteria must be met;

1. there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings;
2. there must be a reasonable expectation of success; and
3. the prior art reference must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

With regard to the invention as recited in claim 1, applicant respectfully submits that a *prima facie* case of obviousness has not been set forth as there has not been shown that any motivation in the cited references exists to determine keys based on the stream identifier as is recited in the claims.

The Manual of Patent Examining Procedure (MPEP) provides further appropriate instruction by which the instant Appeal should be judged. MPEP, Eight Edition, Rev. 2, May 2004, provides in section 2143 entitled: "Fact That The Claimed Invention Is

Within The Capabilities Of One Of Ordinary Skill In The Art Is Not Sufficient By Itself
To Establish *PRIMA FACIE* Obviousness:"

"A statement that modification of the prior art to meet the claimed invention would have been "well within the ordinary skill of the art at the time the claimed invention was made" because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references." *Ex parte Levensgood* 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP §2143.01, p. 2100-131.

Appellant respectfully submits that the references fail to provide motivation to combine their multiple teachings. In this case, it is respectfully submitted that the Office has impermissibly used the teachings of the present invention as a blueprint for selecting and combining the references cited.

For at least the above reasons, Appellant respectfully submits that a case of obviousness has not been set forth.

In view of the above, applicant submits that claim 1 is patentable over the teachings of the cited references.

Rejection of Independent Claims 2, 8, 13 and 18 under 35 USC §103

The rejection of the remaining independent claims is in error because these claims contain subject matter similar to that recited in claim 1, which has been shown not to be rendered obvious by the references cited.

For the remarks made with regard to claim 1, which are reasserted, as if in full, , applicant respectfully submits that the combined teachings of the references cited fails to render obvious the subject matter recited in the remaining independent claims.

In view of the above, applicant submits that the above referred-to claims are patentable over the teachings of the cited references.

Rejection of the Dependent Claims under 35 USC §103

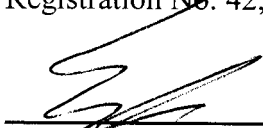
With regard to the dependent claims, these claims are dependent from independent claim 1, Applicant respectfully submits that these claims are allowable at least for their dependence upon allowable base claims, without even contemplating the merits of the dependent claims, as held by *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) (if an independent claim is non-obvious under 35 U.S.C. §103(a), then any claim depending therefrom is non-obvious).

In view of the above, applicant submits that the above referred-to claims are patentable over the teachings of the cited references.

VIII. CONCLUSION

In view of the above analysis, it is respectfully submitted that the referenced teachings, whether taken individually or in combination, fail to render obvious the subject matter of any of the present claims. Therefore, reversal of all outstanding grounds of rejection is respectfully solicited.

Respectfully submitted,
Daniel Piotowski
Registration No. 42,079


By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Date: March 23, 2007

IX. CLAIMS APPENDIX

The claims which are the subject of this appeal are as follows:

1. (Previously presented) A system for copy protecting information, the system comprising:

a point of deployment module; and

a set-top box including;

wherein the set-top box transmits a request message for information, the point of deployment module generates a reply message which includes at least one control information pair, relating to the information, each control information pair having copy control information and a stream identifier, respectively generating a first key in the point of deployment module and a second key in the set-top box, using information associated with each respective device and the at least one control information pair, and the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box, and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match.

2. (Previously presented) A method of copy protecting information transmitted between a deployment module and a host device, the method comprising the steps of:

(a) transmitting a request message for the information from the host device to the deployment module;

(b) transmitting a reply message from the deployment module to the host device, wherein the reply message includes at least one control information pair, each pair having a copy control information and a stream identifier;

(c) generating a first shared key at the host and a second shared key at the deployment module, respectively, using information associated with each respective device and the at least one control information pair and an encryption means;

(d) encrypting, in the deployment module, the information;

(e) transmitting the encrypted information from the deployment module to the host;

(f) decrypting, at the host, the encrypted information; and

(g) receiving the information at the host when the first and second shared keys match.

3. (Original) The method of claim 2, wherein the deployment module is a point of deployment module.

4. (Original) The method of claim 2, wherein the host is a set-top box.

5. (Original) The method of claim 2, wherein the encryption means includes a hash function.

6. (Original) The method of claim 2, wherein the encrypted information in an elementary stream of information is encrypted with the first shared key.

7. (Original) The method of claim 6, wherein the stream identifier that is transmitted to the host is incorporated with the Packetized Elementary Stream (PES) header of the elementary stream.
8. (Previously presented) A deployment module for use with a host device, the deployment module comprising:
- means for communicating with the host device; and
 - a processor for, in response to a request message for information from the host device, generating a reply message to the host device, the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using information associated with the deployment module and the at least one control information pair, encrypting the information with the first shared key and transmitting the encrypted information to the host device.
9. (Original) The deployment module of claim 8, wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer or internet interface appliance.
10. (Original) The deployment module of claim 9, wherein the host device is a set-top box.

11. (Original) The deployment module of claim 10, wherein the encrypted information is transmitted to the host device using a transport stream, wherein the transport stream includes at least one elementary stream.

12. (Original) The deployment module of claim 11, wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams.

13. (Previously presented) A host device for use with a deployment module, the host device comprising:

means for communicating with the deployment module; and

a processor for generating a request message for information to the deployment module, and in response, receiving a reply message from the deployment module, wherein the reply message includes at least one control information pair, each pair having copy control information and a stream identifier, generating a second shared key using information associated with the host device and the at least one control information pair, and decrypting encrypted information, received from the deployment module, with the second shared key, and receiving the information when the second shared key matches a first shared key generated in the deployment module.

14. (Original) The host device of claim 13, wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer or internet interface appliance.

15. (Original) The host device of claim 14, wherein the host device is a set-top box.

16. (Original) The host device of claim 13, wherein the received encrypted information is included in a transport stream, wherein the transport stream includes at least one elementary stream.

17. (Previously Presented) The host device of claim 16, wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams.

18. (Previously presented) An article of manufacture comprising a computer readable medium in which resides a computer program, said article being part of a deployment module for use with a host device, said program comprising:

instruction means for communicating with the host device; and

instructions for, in response to a request message for information from the host device, generating a reply message to the host device, the reply message including at least one control information pair, each pair having copy control information and a stream identifier, generating a first shared key using information associated with the deployment module and the at least one control information pair, encrypting the information with the first shared key and transmitting the encrypted information to the host device.

19. (Previously Presented) The system of claim 1, wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least one control information pair, the respective copy control information of said at least one control information pair not being encrypted for the transmission.

20. (Previously Presented) The method of claim 2, wherein step b) is executed without encrypting said copy control information of said at least one control information pair.

21. (Previously Presented) The deployment module of claim 8, wherein said copy control information of said at least one control information pair in the reply message is unencrypted upon transmission to the host device.

22. (Previously Presented) The deployment module of claim 8, wherein the information to be encrypted comprises content information.

23. (Previously Presented) The deployment module of claim 22, wherein said content information comprises content information of an elementary stream, said stream identifier being an identifier of an elementary stream.

24. (Previously Presented) The system of claim 1, wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information.

25. (Previously Presented) The system of claim 24, wherein said stream identifier is within a Packetized Elementary Stream (PES) header of the elementary stream.

26. (Previously Presented) The system of claim 25, wherein the encrypted information to be transmitted to the set-top box includes said header, said set-top box being configured to retrieve said stream identifier from said header.

27. (Previously Presented) The host device of claim 13, wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information.

28. (Previously Presented) The host device of claim 27, wherein said stream identifier is within a Packetized Elementary Stream (PES) header of the elementary stream.

29. (Previously Presented) The host device of claim 28, wherein the encrypted information to be received includes said header, said host device being configured to retrieve said stream identifier from said header.

30. (Original) The system as recited in claim 1, wherein the information associated with each respective device is a random number generated by each respective device.

X. EVIDENCE APPENDIX

No supplemental evidence was provided by applicant that was entered into the record during the prosecution of this matter.

XI. RELATED PROCEEDING APPENDIX

No related proceedings are pending and, hence, no information regarding same is available.